Binghamton University Foundation
Credit Card Handling Policy

Anyone accepting, processing or handling credit card information on behalf of the Binghamton University Foundation must review and agree to this Credit Card Handling Policy and be approved to have credit card access before handling ANY sensitive credit card information. The policy must be reviewed and agreed to annually.

For the purposes of this document, sensitive credit card information is limited to the full credit card account number (PAN), CAV2/CVC2/CVV2/CID security codes, track information and/or the PIN block. Communications such as "$30 was charged to John's VISA ending in 4266" are not considered to contain sensitive credit card information and would not fall under the scope of this policy.

Credit Card Acceptance:

Only authorized individuals may accept, transport, view or otherwise handle credit card information for the Binghamton University Foundation. Credit card information may never be requested, accepted or transmitted via text message, email, instant message, fax or other electronic messaging technologies. Credit card number received via methods may NOT be processed unless the card information is verified via phone or other acceptable method.

Procedures:

When possible, all credit card transactions should be completed by physically swiping the credit card on an approved, up-to-date dial-out only credit card swipe terminal not connected to the Internet. No sensitive credit card information should be written down or recorded anywhere, and the credit card should be immediately returned to the card holder.

If you do not have access to an approved card swipe terminal, the card holder should, when possible, be referred to an office with an available terminal. This applies to both in person and phone transactions.

If access to a terminal is not immediately available, or referring the card holder to another office is not practical, the credit card information should be phoned in to the appropriate office (i.e. Advancement Services, Accounting Services) for immediate processing, and no sensitive credit card information should be written down.

When absolutely necessary, the minimum required credit card information should be temporarily written on an authorized credit card acceptance form and marked confidential, then processed per the requirements below. Credit Card information which has been written down should be phoned in or physically delivered to the appropriate office for processing by the close of business the day they are received. If same day processing is not possible, the information should be transferred to the appropriate office on the next business day.

PLEASE NOTE: As soon as a document is identified as containing credit card information, it must immediately be handled in accordance with this policy. Only individuals approved to handle credit card information may be placed in a position where they could have visibility to credit card numbers. For example, only individuals approved to handle credit card information may open mail in an office which may receive credit card numbers via postal mail. As soon as the mail is opened and identified as containing a credit card number, that document must be handled per these credit card handling procedures.

Any documents containing credit card information must be marked confidential and always be secured in a locked location, such as a locked desk drawer or filing cabinet accessible only to individuals authorized to handle credit card information. A list of people with access to that location must be maintained and kept up to date. For example, you may not store credit card information in a locked filing cabinet if other, unauthorized department members have access to that filing cabinet. If a locked location is not available, such as when traveling, the credit card information must remain in the possession of the

Binghamton University Foundation
Credit Card Handling Policy

authorized individual at all times, and secured out of view of unauthorized individuals until an appropriate storage location is available.

Any documents containing credit card information must be destroyed via cross-cut shredding as soon as the information is transferred to the appropriate office for processing or the transaction is completed, whichever comes first. If shredding of the entire document is not possible, the portion containing the credit card information should be cut-off and shredded. Documents should be designed with this procedure in mind. For existing documents where this is not possible, credit card information must be blacked out using a black, broad-tip permanent marker rendering it illegible, the original document copied and the original destroyed by crosscut shredding.

Communication Methods:

- ONLY communicate credit card information via phone or hand deliver. Do NOT send via email, chat, text or any other end-user messaging methods. Do NOT fax credit card information.
- ONLY write credit card information on approved, properly labelled confidential credit card forms.
- ONLY store credit card information until it has been processed. Immediately destroy credit card numbers via cross cut shredding as soon as they are processed (cards should be processed the day they are received)

- DO NOT send credit card information through the mail. This includes campus mail, USPS, FedEx, UPS, etc. These are NOT considered secure communication methods and may NOT be used to transfer credit card information.
- DO NOT send credit card transaction paperwork with a student worker or other unauthorized individual. Only individuals authorized to access credit card information may be used to transfer credit card information.
- DO NOT type credit card numbers into your computer for **any** reason. This includes typing them into your computer "just to print out a legible copy", entering them into a website, etc.
- DO NOT allow a cardholder to use your computer to enter a transaction into our online giving site.
- DO NOT process any transaction on behalf of a donor/attendee using the online giving or event registration sites.
- DO NOT email, text, chat, instant message, fax, etc. credit card information.
- DO NOT store credit card numbers "until you have several to process". Credit cards should be processed immediately. If the number was written down, destroy the document immediately after processing.
- DO NOT store credit card numbers in spreadsheets, word documents, etc.

Storage of Credit Card Information:

Sensitive credit card data may never be stored in any format long term; this includes paper, electronic and audio (i.e. voice messages). It is NOT acceptable to store full credit card numbers for any reason including, but not limited to, recurring charges, security deposits or potential purchases.

Exception: The Advancement Services office may store the full credit card number, cardholder name and expiration date on a physical paper secured in a designated safe accessible only by authorized Advancement Services staff for a period of time necessary to complete recurring credit card charges as authorized and requested by the card holder. The duration of these charges must be documented and reviewed at least annually, and all documents containing credit card information related to completed recurring contracts must be destroyed via cross-cut shred or the credit card information rendered unreadable by thorough blotting out with a black permanent marker, photocopying the document then destroying the original.

Binghamton University Foundation
Credit Card Handling Policy

Credit Card Swipe Terminals / Credit Card Processing:

Only approved University or Foundation employees may process credit card transactions or otherwise have direct access to a credit card swipe terminal, online credit card processing account or voice authorization. Employees authorized to process transactions must ALSO review and agree to the Binghamton University Foundation Credit Card Processing Policy.

Administrative Responsibilities:

Any security incidents or concern related to the security or handling of sensitive credit card data must be reported to the Senior Director of Administrative Services for the Foundation immediately. For any employee related credit card handling concerns, please refer to your employee manual for appropriate reporting procedures.

The Senior Director of Administrative Services for the Foundation is responsible for approving all requests for authorization for access to sensitive credit card information.

The Foundation's Accounting Services department will be responsible for maintaining an up-to-date list of all personnel authorized for access to sensitive credit card information. All individuals will be required to review and agree to the Credit Card Handling Policy at least once per year.

All service providers and/or 3rd party vendors who will have access to sensitive credit card information must be approved by the Senior Director of Administrative Services for the Foundation and will be added to a list of service providers maintained by the Foundation's Accounting Services department. All such service providers will be required to prove to the Accounting Services office that they are PCI Compliant at all times. Contracts with any service provider that will have access to sensitive credit card information must be maintained that specifically states that the vendor acknowledges they are responsible for the security of cardholder data the service provider possesses.

_____	_____	_____
Requestor's Signature	Requestor's Name (Printed)	Date
_____	_____	_____
Requestor's Department	Binghamton Email Address	Phone/Extension

NEW AUTHORIZATIONS ONLY

_____	_____	_____
BNumber (New hires only)	Hire Date (New hires only)	Type (State or RF)
_____	_____	_____
Supervisor's Signature	Supervisor's Name (Printed)	Date
_____	_____	_____
Authorized Signature (Foundation Acct Svcs)	Authorized Name (Printed)	Date